Supreme Court, U.S.
FILED
2007
OFFICE OF THE CLERK

No. _____

In The

Supreme Court of the United States

CHRISTOPHER ANDREW PHILLIPS,

Petitioner,

v.

THE UNITED STATES OF AMERICA,

Respondent.

On Petition For A Writ Of Certiorari To The United States Court Of Appeals For The Fifth Circuit

PETITION FOR A WRIT OF CERTIORARI

TERRENCE W. KIRK
Texas Bar No. 11513500
600 West 13th Street
Austin, Texas 78701
(512) 236-8511
(512) 476-5346 (Fax)
Counsel for Petitioner

COCKLE LAW BRIEF PRINTING CO. (800) 225-6964
OR CALL COLLECT (402) 342-2831

QUESTION PRESENTED

WHERE A DEFENDANT DOES NOT OBJECT TO A CONSTRUCTIVE AMENDMENT AT TRIAL, MUST PREJUDICE ALWAYS BE SHOWN UNDER THE PLAIN ERROR DOCTRINE?

TABLE OF CONTENTS

	Page
QUESTION PRESENTED	i
TABLE OF AUTHORITIES	iii
OPINIONS BELOW	1
STATEMENT OF JURISDICTION	1
CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED	2
STATEMENT OF THE CASE	2
REASONS FOR GRANTING THE PETITION	6
ARGUMENT	6
CONCLUSION	15

INDEX TO APPENDICES

APPENDIX A	Opinion of the Fifth Circuit Court of Appeals affirming Petitioner's conviction	1a
APPENDIX B	Judgment of United States District Court for the Western District of Texas	18a
APPENDIX C	Order of Fifth Circuit denying Petition for Rehearing *En Banc*	29a

TABLE OF AUTHORITIES

Page

CASES

International Airport Centers, L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006) 14

Stirone v. United States, 361 U.S. 212 (1960) 6, 7, 10, 12,14

United States v. Brown, 400 F.3d 1242 (10th Cir. 2005) 12

United States v. Cotton, 535 U.S. 625 (2002) 6, 11, 12, 13, 15

United States v. Daniels, 252 F.3d 411 (5th Cir. 2006), *cert. denied*, 535 U.S. 1095 (2002) 11, 15

United States v. DiCicco, 439 F.3d 36 (1st Cir. 2006) 8

United States v. Floresca, 38 F.3d 706 (4th Cir. 1994) (*en banc*) 7, 8, 11

United States v. McGilberry, 480 F.3d 326 (5th Cir. 2007) 14, 15

United States v. Miller, 471 U.S. 130 (1985) 14

United States v. Morris, 928 F.2d 504 (2d Cir. 1991) 14

United States v. Olano, 507 U.S. 725 (1993) 8, 10

United States v. Reyes, 102 F.3d 1361 (5th Cir. 1996) 9, 10

United States v. Syme, 276 F.3d 131 (3d Cir. 2002) 8, 10

United States v. Thomas, 274 F.3d 655 (2d Cir. 2001) 6, 7

TABLE OF AUTHORITIES – Continued

Page

CONSTITUTIONAL PROVISIONS

U.S. CONST. amend. V 2, 14

STATUTORY PROVISIONS

18 U.S.C. § 1030(a)(5)(A)(i) 2, 4

18 U.S.C. § 1030(a)(5)(A)(ii) 2, 4

28 U.S.C. § 1254(1) 2

RULES

FED. R. CRIM. P. 52(a) 7

FED. R. CRIM. P. 52(b) 10

SUP. CT. R. 10(a) 6

SUP. CT. R. 10(c) 6

SUP. CT. R. 13(3) 1

PETITION FOR A WRIT OF CERTIORARI

TO THE HONORABLE JUSTICES OF THE SUPREME COURT:

COMES NOW Petitioner Christopher Andrew Phillips, by and through his undersigned counsel, and respectfully requests the Court to grant his petition for a writ of certiorari to review the decision of the United States Court of Appeals for the Fifth Circuit affirming his conviction for unauthorized access to a protected computer. In support, Petitioner offers the following:

OPINIONS BELOW

Petitioner was convicted in the United States District Court for the Western District of Texas and sentenced to five years of probation. The judgment of the trial court is attached to this petition as Appendix B. On January 24, 2007, the United States Court of Appeals for the Fifth Circuit, in an opinion authored by Chief Judge Edith Jones and joined by Judges Smith and Stewart, affirmed Petitioner's conviction in a published opinion, *United States v. Phillips*, 477 F.3d 215 (5th Cir. 2007) (Appendix A). On March 1, 2007, the Fifth Circuit allowed the untimely filing of a petition for rehearing *en banc*, but denied it. (Appendix C).

STATEMENT OF JURISDICTION

Pursuant to Rule 13(3) of the Rules of this Court, Petitioner has ninety days from March 1, 2007, the date his petition for rehearing *en banc* was denied, to file this

petition. This petition is being filed by May 30, 2007, ninety days from the date the petition for rehearing *en banc* was denied. Jurisdiction is proper under 28 U.S.C. § 1254(1).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

The Fifth Amendment to the United States Constitution provides, in pertinent part, "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury . . . "

18 U.S.C. § 1030(a)(5)(A)(i) provides, in pertinent part, that whoever "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage to a protected computer . . . shall be punished as provided in subsection (c) of this section."

18 U.S.C. § 1030(a)(5)(A)(ii) provides, in pertinent part, that whoever "intentionally accesses a protected computer without authorization, and as a result of such conduct causes damage . . . shall be punished as provided in subsection (c) of this section."

STATEMENT OF THE CASE

A. Statement of Facts

The relevant facts, as the Fifth Circuit saw them, are summarized in the panel's opinion:

Petitioner designed a computer program expressly for the purpose of hacking into the UT system via a portal known as the "TXClass Learning Central: a Complete Training Resource for UT Faculty and Staff." TXClass was a "secure" server operated by UT and used by faculty and staff as a resource for enrollment in professional education courses. Authorized users gained access to their TXClass accounts by typing their Social Security numbers in a field on the TXClass website's log-on page. Phillips exploited the vulnerability inherent in this log-on protocol by transmitting a "brute-force attack" program[1] which automatically transmitted to the website as many as six Social Security numbers per second, at least some of which would correspond to those of authorized TXClass users.

Initially, Phillips selected ranges of Social Security numbers for individuals born in Texas. But he refined the brute-force attack to include only numbers assigned to the ten most populous Texas counties. When the program hit a valid Social Security number and obtained access to TXClass, it automatically extracted personal information corresponding to that number from the TXClass database and, in effect, provided Phillips a "back door" into UT's main server and unified database. Over a fourteen-month period, Phillips thus gained access to a mother lode of data about more than 45,000 current and prospective students, donors, and alumni.

---

[1] As will be seen, the Fifth Circuit is simply wrong in asserting that Petitioner "transmitted" a "program" to a UT computer. While Petitioner ran a program on *his* computer, he never transmitted it to run on a UT computer.

> Phillip's actions hurt the UT computer system. The brute-force attack program proved so invasive – increasing the usual monthly number of unique requests received by TXClass from approximately 20,000 to as many as 1,200,000 – that it caused the UT computer system to crash several times in early 2003.

Id. at 477 F.3d 218 (Footnote omitted).

B. Statement of Procedural History

Petitioner was indicted on November 3, 2004, in a four-count indictment. The jury acquitted Petitioner on two counts that required an intent to defraud and the trial court, the Honorable Lee Yeakel, Judge Presiding, granted a motion to dismiss count four on the basis that such a conviction would violate the Ex Post Facto Clause. Subsequently, on September 6, 2005, the court conducted a sentencing hearing. Rejecting the Government's plea for a sentence of imprisonment, the court sentenced Petitioner to five years on probation and ordered him to pay $170,056 in restitution to the University of Texas.

On appeal, Petitioner contended, *inter alia*, that the trial court had constructively amended the indictment, count one of which charged him with intentionally accessing a protected computer. The panel hearing the appeal agreed that this was a "classic constructive amendment," but nevertheless affirmed Petitioner's conviction on the ground that he had not shown prejudice, as required by the plain error doctrine. *United States v. Phillips*, 477 F.3d 215, 222-223 (5th Cir. 2007).

C. Summary of the Issue

Petitioner was indicted for intentionally accessing a protected computer, as proscribed by 18 U.S.C. § 1030(a)(5)(A)(ii). The district court's charge, however, allowed a conviction based on 18 U.S.C. § 1030(a)(5)(A)(i), which applies to anyone who "knowingly *causes the transmission of a program* . . . to a protected computer." (Emphasis added). The panel found that the instruction "plainly modified an essential element of the charged offense by supporting the act of accessing a protected computer under subsection (ii) on the basis of transmitting a program under subsection (i)." *Phillips*, *supra*, at 477 F.3d 222. According to the court, this "was a classic constructive amendment." *Id.*

Since Petitioner did not object to the instruction, however, the court applied the plain error standard of review. Under this standard, the court found that Petitioner had not shown prejudice even though the instruction allowed a conviction on a different act than the one specified in the indictment, and even though the instruction did not "fully convey that the jury must find that [Petitioner] acted intentionally without authorization." *Id.* at 477 F.3d 223. The court reasoned that the jury could not have concluded that Petitioner transmitted the program "without having also accessed a protected computer," and that because he transmitted the program, the jury must have also found that he intended not only to access the computer, but that the access be unauthorized.[2] *Id.*

---

[2] Whether Petitioner acted "without authorization" was a key issue in the case, with the other issues being whether he had any intent to defraud and whether he knew he was damaging the UT System.

REASONS FOR GRANTING THE PETITION

1. The Fifth Circuit's decision conflicts with the decisions of the Second, Third, and Fourth Circuit Courts of Appeals. SUP. CT. R. 10(a).

2. The Fifth Circuit's decision conflicts with a relevant decision of this Court, i.e., *United States v. Cotton*, 535 U.S. 625 (2002). SUP. CT. R. 10(a).

3. How the plain error doctrine should be applied to constructive amendments is an important question of federal law that has not been settled by this Court. SUP. CT. R. 10(c).

ARGUMENT

The first reason to grant this petition is the conflict between the approach of the Fifth Circuit in this case and the analysis employed by the Second, Third, and Fourth Circuit Courts of Appeals. In *United States v. Thomas*, 274 F.3d 655 (2d Cir. 2001) (*en banc*), the Second Circuit held that a "constructive amendment is a *per se* prejudicial violation of the Grand Jury Clause of the Constitution . . . " *Id.* at 274 F.3d 670. In so holding, the court rested its decision on prior precedent from this Court:

> Our rule that a constructive amendment is per se prejudicial is grounded in the recognition that "[t]he very purpose of the requirement that a man be indicted by grand jury is to limit his jeopardy to offenses charged by a group of his fellow citizens acting independently of either prosecuting attorney *or* judge." *Stirone v. United States*, 361 U.S. 212, 218, 80 S. Ct. 270, 4

> L. Ed. 2d 252 (1960) (emphasis added). Indeed, a grand jury "belongs to no branch of the institutional Government," but rather "serv [es] as a kind of buffer or referee between the Government and the people." *United States v. Williams*, 504 U.S. 36, 47, 112 S. Ct. 1735, 118 L. Ed. 2d 352 (1992). Thus, it would be inappropriate for a court to speculate as to whether a grand jury might have returned an indictment in conformity with the available evidence, because such an exercise would work the harm the Grand Jury Clause is intended to prevent – a federal prosecution begun by arms of the Government without the consent of fellow citizens. *Cf. Stirone*, 361 U.S. at 217-19 ("The grand jury which found this indictment was satisfied to charge that Stirone's conduct interfered with interstate importation of sand. But neither this nor any other court can know that the grand jury would have been willing to charge [the theory upon which the conviction rested, namely] that Stirone's conduct would interfere with interstate exportation of steel from a mill later to be built with Rider's concrete.").

Id.

The Fourth Circuit has gone even further, ruling that constructive amendments constitute plain error *per se*. *United States v. Floresca*, 38 F.3d 706 (4th Cir. 1994) (*en banc*). The *Floresca* court also relied on this Court's decision in *Stirone*: because Rule 52(a), the plain error rule, applies only to an error "which does not affect substantial rights," the Fourth Circuit observed, *Stirone* necessarily dictates that a constructive amendment must always affect "substantial rights." *Floresca* at 38 F.3d 713. In

addition, the Fourth Circuit declared that its decision was fully consistent with *United States v. Olano*, 507 U.S. 725 (1993), the leading case from this Court on the plain error doctrine. *See also United States v. DiCicco*, 439 F.3d 36, 44-45 (1st Cir. 2006) (Stating in *dicta* that constructive amendments are plain error *per se*).

Similarly, the Third Circuit in *United States v. Syme*, 276 F.3d 131 (3d Cir. 2002), read *Olano* to mean that while a defendant must ordinarily show prejudice if he did not object at trial, constructive amendments fall into the *Olano* "category of errors" that "should be presumed prejudicial if the defendant cannot make a specific showing of prejudice." *Syme* at 276 F.3d 154, quoting from *Olano* at 507 U.S. 735. Accordingly, the law in the Third Circuit is that constructive amendments create a rebuttable presumption of prejudice. *Syme* at 276 F.3d 153. Unlike the law in the Second and Fourth Circuits, however, the Third Circuit presumption is rebuttable, and a reviewing court must still decide whether the constructive amendment seriously affected "the fairness and integrity of the trial." *Syme* at 276 F.3d 155.

Petitioner maintains that the Fifth Circuit's approach is flawed, for two reasons. First, the Fifth Circuit in this case focused on what the jury would have (in its view) decided if correctly instructed. As noted in *Floresca*, however, the substantial right at issue is the right to be charged by the *grand jury*, and just as defendants are not entitled to speculate on the basis for an indictment, the Government should not be allowed to argue that a grand jury would have indicted under a particular theory had the

theory been presented to them.[3] It is up to the Government to indict the defendant before trial, not at the end of it.

Second, the Fifth Circuit rule is largely predicated on the notion that a defendant may "sandbag" a trial court by deliberately failing to object. *See, e.g., United States v. Reyes*, 102 F.3d 1361, 1366 (5th Cir. 1996). The panel opinion here does not intimate that Petitioner did that here, however; it is just as believable to speculate that the Government deliberately submitted the charge to gain an unfair advantage by changing the focus of the case from the authorization issue to the damage issue. "Why the Government overlooked the inconsistency between the statutory provision cited in the indictment and the provision described in the jury charge is a mystery." *Phillips, supra,* at 477 F.3d 222.

More fundamentally, however, the Third Circuit has refuted the fears about "sandbagging":

> We recognize that the presumption that we apply, like any exception to the general rule that the burden is on the defendant to demonstrate all of the prongs of the plain error test, may increase the likelihood of defendants "sandbagging," i.e., failing to object to an error at the trial level in order to keep an issue for appeal as insurance in the event they are convicted. The Fifth Circuit cited its concerns about sandbagging as the reason for its refusal to notice plain error in the constructive amendment context. See

[3] Although the indictment here included the word, "program," it did not define the term, nor the word, "access." And in charging the offense of "accessing," the grand jury did not claim that Petitioner did so by "transmitting" anything.

> *Reyes*, 102 F.3d at 1365. There are, however, two reasons why the potential instances of sandbagging arising from the presumption that we apply today will be limited. First, constructive amendments are a narrowly defined category of errors, which arise relatively infrequently. The presumption of prejudice under plain error analysis does not extend to the more frequently encountered category of variances from an indictment, which may be dismissed as harmless even when properly objected to at trial. See, e.g. *[United States vs.] Castro, 776 F.2d at 1121 & n.* (Distinguishing constructive amendments from variances). Second, even with a presumption of prejudice in plain error analysis of constructive amendments, defendants who may be considering a sandbagging strategy still risk that an appellate court will exercise its discretion to refuse to notice plain error if the defendant fails to object to the error at the trial level. See *Fed.R.Crim.P. 52(b)* ("Plain errors or defects affecting substantial rights *may* be noticed although they were not brought to the attention of the court.") (emphasis added); see also *Olano*, 507 U.S. at 732, 113 S. Ct. 1770 (noting that appellate courts are not required to notice plain error, but may do so at their discretion). Appellate courts will be particularly reluctant to notice a constructive amendment as plain error if they suspect that the defendant was sandbagging).

United States v. Syme, *supra*, at 276 F.3d 154, note 9.

In short, the panel decision conflicts with the decisions of the Second, Third, and Fourth Circuits, and appears to misinterpret the effect of *Olano* on *Stirone*. This Court should agree to resolve what is essentially a four-way split in the circuit courts.

A second reason for granting the petition is to examine the effect of this Court's decision in *United States v. Cotton*, *supra*, on plain error analysis. Several years ago, in *United States v. Daniels*, 252 F.3d 411 (5th Cir. 2001), *cert. denied*, 535 U.S. 1095 (2002), this Court refused to grant review on the issue here, most likely because, as argued in the Government's Brief in Opposition, no constructive amendment occurred in that case.

The Government also pointed out in *Daniels*, however, that this Court had granted certiorari in *Cotton*, and that *Cotton* might "shed light on constructive amendment claims raised for the first time on appeal, effectively resolving any conflict between the approach taken in *Floresca* and the approach taken by the Fifth Circuit . . . " Brief for the United States in Opposition, at p. 6, note 2.

Since then, at least one court has accepted the Government's argument. In rejecting a plain error claim two years ago, the Tenth Circuit said that constructive amendment claims no longer constituted reversible error *per se* because of *Cotton*:

> Tenth Circuit precedent establishes some uncertainty as to whether a constructive amendment of an indictment by jury instructions to which the defendant did not object is reversible per se or reversible only where the amendment constitutes plain error and seriously affects the fairness, integrity or public reputation of judicial proceedings. Compare *United States v. Levine*, 41 F.3d 607, 617 n.13 (10th Cir. 1994) (reversible per se) with *United States v. Cavely*, 318 F.3d 987, 999 (10th Cir. 2003) (applying plain error standard without citing *Levine*. After *Levine* but before *Cavely*, the Supreme Court decided *United States v. Cotton*, 535 U.S. 625, 122 S. Ct. 1781,

> 152 L. Ed. 2d 860 (2002). In *Cotton*, the Court declined to notice plain error in a situation where the indictment lacked any reference to threshold drug quantities, a defect of constitutional magnitude after *Apprendi v. New Jersey*, 530 U.S. 466, 120 S. Ct. 2348, 147 L. Ed. 2d (2000).
>
> See id. at 627-28, 122 S. Ct. 1781. The indictment alone would have yielded a maximum sentence of twenty years, yet the defendants were sentenced to at least ten years above the maximum due to the district court's finding of 500 or more grams of cocaine base. Id. Because the defendants had not objected below, the Court engaged in plain error review. Id. at 631, 122 S. Ct. 1781 (distinguishing *Stirone v. United States*, 361 U.S. 212, 80 S. Ct. 270, 4 L. Ed. 2d 252 (1960), on basis that constructive amendment claim there was raised in district court); see also 3 CHARLES ALLEN WRIGHT ET AL., FEDERAL PRACTICE & PROCEDURE: CRIMINAL 3D § 516 at 51 & n.16. Although there was constitutional error that was plain and resulted in substantially increased sentences for the defendants, the Court upheld the sentences because the uncharged drug quantity was supported by overwhelming and uncontroverted evidence. *Cotton*, 535 U.S. at 634, 122 S. Ct. 1781. The Court ruled the "fairness, integrity and public reputation of judicial proceedings" would be threatened if the sentence were overturned. Id. It is clear, therefore, that the automatic reversal rule of *Levine* no longer applies in a constructive amendment plain error case, i.e., where the defendant failed to object in the district court.

United States v. Brown, 400 F.3d 1242, 1254, note 6 (10th Cir. 2005).

While it is true that the *Cotton* Court ruled that even a right as fundamental as the Fifth Amendment grand jury right could be forfeited by inaction, *Cotton* at 535 U.S. 634, this Court should recognize that the Fifth Circuit's approach in this case actually conflicts with *Cotton's* analysis. In *Cotton*, this Court did not reach the issue of whether prejudice had to be shown, but held only that the fourth prong of the plain error test was not satisfied because the evidence as to the charged offense was "overwhelming." *Id.* at 520 U.S. 469-470.

By contrast, the Fifth Circuit in this case held that Petitioner had not shown prejudice, i.e., that his substantial rights were not affected – the third prong of the plain error test. Moreover, although the court found that the evidence was sufficient to prove that Petitioner intentionally accessed the UT computer system, as the grand jury had charged, *Phillips* at 477 F.3d 219-221, the evidence of this was certainly not "overwhelming" or "essentially uncontested." As reflected in the opinion, and vigorously argued both at trial and on appeal, Petitioner maintained that because the TXClass website was a "public application" not requiring any special password, UT had not given sufficient notice that access was unauthorized.

Moreover, whether the constructive amendment here should be deemed plain error depends upon another factor not recognized by the Fifth Circuit – the fact that the jury charge actually given was not only based on an uncharged offense, but was not itself supported by the evidence. In its opinion, the court declared that Petitioner exploited the UT system by "transmitting a brute-force attack program," *id.* at 477 F.3d 218, and justified its holding on the basis that the "factual predicates" for the conviction under both the indictment and the jury charge were "identical":

"knowingly transmitting a program and intentionally accessing a protected computer." *Id.* at 477 F.3d 222.

But while the court refers to a "brute force attack" as a "term of art" to describe a specific type of program, *Phillips* at 477 F.3d 218, note 2, the court provides no authority for its assumption that Petitioner "transmitted" the program. What the court fails to see is that this was not a case like *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991), cited in the Fifth Circuit's opinion, where the defendant actually "transmitted" a program – a "worm" – to other computers. *See also International Airport Centers L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006) (Employee "transmitted" program by installing a "secure-erasure" program on employer's computer). Petitioner did not "transmit" any "program," and would have been entitled to an acquittal had he been charged with such an offense. Similarly, had the grand jury been presented with the applicable law, it would not have indicted Petitioner for "transmitting" a program.

The upshot of all this is that Petitioner was convicted of "accessing" based on the act of "transmitting" – but without proof that he "transmitted." This was not just a case of the Government charging one theory and proving another, as in *Stirone*, but of charging one theory and *not* proving the different theory submitted to the jury. *Cf. United States v. McGilberry,* 480 F.3d 326 (5th Cir. 2003) (Finding that constructive amendment did not affect fairness of proceeding where it *narrowed* the basis on which defendant could have been convicted); *United States v. Miller*, 471 U.S. 130 (1985) (Fifth Amendment not violated where Government abandoned one of two theories alleged in indictment).

In sum, unlike the case in *Daniels*, this is the ideal time to settle an important question of federal law – how the plain error doctrine should apply to constructive amendments. *Cotton* did not decide this question, the circuit courts are in disarray, and the Fifth Circuit itself adopted one approach to the question in January of this year (Petitioner's case) (Requiring a showing of prejudice) and another the next month (*McGilberry*) (Not deciding prejudice issue, but looking to fourth prong). If it is not time for a bright-line rule, it is time for some kind of rule.

CONCLUSION

Petitioner requests that this Court grant his petition for a writ of certiorari.

Respectfully submitted,

TERRENCE W. KIRK
State Bar No. 11513500
600 West 13th Street
Austin, Texas 78701
(512) 236-8511
(512) 476-5346 (Fax)
Counsel for Petitioner

477 F.3d 215

United States Court of Appeals, Fifth Circuit.
UNITED STATES of America, Plaintiff-Appellee,
v.
Christopher Andrew PHILLIPS,
Defendant-Appellant.
No. 05-51271.

Jan. 24, 2007.

Joseph H. Gay, Jr., Asst. U.S. Atty., Mark Twain Roomberg (argued), San Antonio, TX, for Plaintiff-Appellee.

Terrence W. Kirk (argued), Austin, TX, for Defendant-Appellant.

Appeal from the United States District Court for the Western District of Texas.

Before JONES, Chief Judge, and SMITH and STEWART, Circuit Judges.

EDITH H. JONES, Chief Judge:

Christopher Andrew Phillips ("Phillips") appeals his conviction for intentionally accessing a protected computer without authorization and recklessly causing damage in excess of $5,000, pursuant to the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. §§ 1030(a)(5)(A)(ii) and (B)(i). Phillips alleges that (1) insufficient evidence was presented at trial to support his conviction under § 1030(a)(5)(A)(ii); (2) the district court's jury charge constructively amended the indictment; (3) the district court's failure to include a lesser-included offense instruction in the jury charge was error; and (4) the district court's award of over $170,000 in restitution under 18 U.S.C. § 3663A was erroneous. Finding no reversible error, we AFFIRM.

I. BACKGROUND

Phillips entered the University of Texas at Austin ("UT") in 2001 and was admitted to the Department of Computer Sciences in 2003. Like all incoming UT students, Phillips signed UT's "acceptable use" computer policy, in which he agreed not to perform port scans using his university computer account.[1] Nonetheless, only a few weeks after matriculating, Phillips began using various programs designed to scan computer networks and steal encrypted data and passwords. He succeeded in infiltrating hundreds of computers, including machines belonging to other UT students, private businesses, U.S. Government agencies, and the British Armed Services webserver. In a matter of months, Phillips amassed a veritable informational goldmine by stealing and cataloguing a wide variety of personal and proprietary data, such as credit card numbers, bank account information, student financial aid statements, birth records, passwords, and Social Security numbers.

The scans, however, were soon discovered by UT's Information Security Office ("ISO"), which informed Phillips on three separate occasions that his computer had been detected portscanning hundreds of thousands of

---

[1] Port scanning is a technique used by computer hackers by which an individual sends requests via a worm or other program to various networked computer ports in an effort to ascertain whether particular machines have vulnerabilities that would leave them susceptible to external intrusion. Often used as an initial step in launching an attack on another computer or transmitting a virus, port scanning is a relatively unsophisticated, but highly effective, reconnaissance method, likened at trial by UT's information technology chief as the electronic equivalent of "rattling doorknobs" to see if easy access can be gained to a room.

external computers for vulnerabilities. Despite several instructions to stop, Phillips continued to scan and infiltrate computers within and without the UT system, daily adding to his database of stolen information.

At around the time ISO issued its first warning in early 2002, Phillips designed a computer program expressly for the purpose of hacking into the UT system via a portal known as the "TXClass Learning Central: A Complete Training Resource for UT Faculty and Staff." TXClass was a "secure" server operated by UT and used by faculty and staff as a resource for enrollment in professional education courses. Authorized users gained access to their TXClass accounts by typing their Social Security numbers in a field on the TXClass website's log-on page. Phillips exploited the vulnerability inherent in this log-on protocol by transmitting a "brute-force attack" program,[2] which automatically transmitted to the website as many as six Social Security numbers per second, at least some of which would correspond to those of authorized TXClass users.

Initially, Phillips selected ranges of Social Security numbers for individuals born in Texas, but he refined the brute-force attack to include only numbers assigned to the ten most populous Texas counties. When the program hit a valid Social Security number and obtained access to TXClass, it automatically extracted personal information corresponding to that number from the TXClass database and, in effect, provided Phillips a "back door" into UT's

---

[2] "Brute-force attack" is term of art in computer science used to describe a program designed to decode encrypted data by generating a large number of passwords.

main server and unified database. Over a fourteen-month period, Phillips thus gained access to a mother lode of data about more than 45,000 current and prospective students, donors, and alumni.

Phillips's actions hurt the UT computer system. The brute-force attack program proved so invasive-increasing the usual monthly number of unique requests received by TXClass from approximately 20,000 to as many as 1,200,000 – that it caused the UT computer system to crash several times in early 2003. Hundreds of UT web applications became temporarily inaccessible, including the university's online library, payroll, accounting, admissions, and medical records. UT spent over $122,000 to assess the damage and $60,000 to notify victims that their personal information and Social Security numbers had been illicitly obtained.

After discovering the incursions, UT contacted the Secret Service, and the investigation led to Phillips. Phillips admitted that he designed the brute-force attack program to obtain data about individuals from the UT system, but he disavowed that he intended to use or sell the information.

Phillips was indicted and convicted after a jury trial on one count of computer fraud pursuant to 18 U.S.C. § 1030(a)(5)(A)(ii) and (B)(i), and one count of possession of an identification document containing stolen Social Security numbers pursuant to 18 U.S.C. § 1028(a)(6). Phillips timely filed a motion for judgment of acquittal challenging, unsuccessfully, the sufficiency of the evidence regarding the loss amount used to support the computer fraud

conviction, and asserting, correctly, that his conviction under § 1028(a)(6) violated the Ex Post Facto Clause.[3] He was sentenced to five years' probation, five hundred hours of community service, and restitution of $170,056. Phillips appealed.

II. DISCUSSION

A. Sufficiency of the Evidence

Phillips asserts that the Government failed to produce sufficient evidence that he "intentionally access[ed] a protected computer without authorization" under § 1030(a)(5)(A)(ii).

Although Phillips timely filed a motion for judgment of acquittal, *see* Fed.R.Crim.P. 29, the motion raised only the narrow issue whether the loss or damage caused by his online exploits exceeded $5,000.00. *See* § 1030(a)(5)(B)(i). Both the Government's opposition memorandum and the district court's ruling on the motion addressed this one issue. Accordingly, "[w]here, as here, a defendant asserts *specific grounds* for a specific element of a specific count for a Rule 29 motion, he waives all others for that specific count." *United States v. Herrera,* 313 F.3d 882, 884 (5th Cir.2002) (en banc), *cert. denied,* 537 U.S. 1242, 123 S.Ct. 1375, 155 L.Ed.2d 213 (2003) (emphasis in original). We thus review his newly raised claim that there was insufficient

[3] Section 1023(a)(6) was amended on April 30, 2003, by adding the phrase "knowingly possesses an authentication feature of the United States which is stolen." Because the last act Phillips committed that would qualify for punishment under this provision occurred on March 2, 2003, the district court correctly dismissed the conviction under this count as violative of the Ex Post Facto clause, U.S. Const. art. I, § 9.

evidence of the statutorily required mens rea under § 1030(a)(5)(A)(ii) only for a "manifest miscarriage of justice." *United States v. Green,* 293 F.3d 886, 895 (5th Cir.2002) (internal quotation marks omitted). Under this exacting standard of review, a claim of evidentiary insufficiency will be rejected unless "the record is devoid of evidence pointing to guilt" or if the evidence is "so tenuous that a conviction is shocking." *United States v. Avants,* 367 F.3d 433, 449 (5th Cir.2004).

Phillips's insufficiency argument takes two parts: that the Government failed to prove (1) he gained access to the TXClass website without authorization and (2) he did so intentionally.

With regard to his authorization, the CFAA does not define the term, but it does clearly differentiate between unauthorized users and those who "exceed[] authorized access." *See* § 1030(e)(6) (defining "exceeding authorized access" as "access[ing] a computer with authorization and . . . us[ing] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter . . . "); *see also* §§ 1030(a)(1), (a)(2), (a)(4). Several subsections of the CFAA apply exclusively to users who lack access authorization altogether. *See, e.g.,* §§ 1030(a)(3), (5)(A)(i), (5)(A)(ii), (5)(A)(iii). In conditioning the nature of the intrusion in part on the level of authorization a computer user possesses, Congress distinguished between "insiders, who are authorized to access a computer," and "outside hackers who break into a computer." *See* S.Rep. No. 104-357, at 11 (1996); *see also* S.Rep. No. 99-432, at 10, *as reprinted in* 1986 U.S.C.C.A.N. 2479, at 2488 (1986) (stating that §§ 1030(a)(3) and (a)(5) "will be aimed at 'outsiders' ").

Courts have therefore typically analyzed the scope of a user's authorization to access a protected computer on the basis of the expected norms of intended use or the nature of the relationship established between the computer owner and the user. Applying such an intended-use analysis, in *United States v. Morris,* 928 F.2d 504 (2d Cir.1991), a case involving an invasive procedure that prefigured modern portscanning, the Second Circuit held that transmission of an internet worm designed "to demonstrate the inadequacies of current security measures on computer networks by exploiting . . . security defects" was sufficient to permit a jury to find unauthorized access within the meaning of § 1030(a)(5)(A). *Morris,* 928 F.2d at 505. The *Morris* court determined that conduct, like "password guessing" or finding "holes in . . . programs," that uses computer systems not "in any way related to their intended function" amounts to obtaining unauthorized access. *Id.* at 510; *see also Creative Computing v. Getloaded.com LLC,* 386 F.3d 930 (9th Cir.2004) (internet site administrator's misappropriation of login names and passwords to obtain access to competitor's website violated CFAA); *Theofel v. Farey-Jones,* 359 F.3d 1066, 1074 (9th Cir.), *cert. denied,* 543 U.S. 813, 125 S.Ct. 48, 160 L.Ed.2d 17 (2004) (use of an authorized third-party's password by an outside hacker to gain access to a mail server fell within "the paradigm of what [Congress] sought to prohibit [under the Stored Communications Act]"); *EF Cultural Travel BV v. Explorica, Inc.,* 274 F.3d 577, 582 n. 10 (1st Cir.2001) (mentioning in dicta the district court's observation of a "default rule" that conduct is unauthorized for § 1030 purposes "if it is not in line with reasonable expectations of the website owner and its users") (internal quotation marks omitted).

Phillips's brute-force attack program was not an intended use of the UT network within the understanding of any reasonable computer user and constitutes a method of obtaining unauthorized access to computerized data that he was not permitted to view or use. During cross-examination, Phillips admitted that TXClass's normal hourly hit volume did not exceed a few hundred requests, but that his brute-force attack created as many as 40,000. He also monitored the UT system during the multiple crashes his program caused, and backed up the numerical ranges of the Social Security numbers after the crashes so as not to omit any potential matches. Phillips intentionally and meticulously executed both his intrusion into TXClass and the extraction of a sizable quantity of confidential personal data. There was no lack of evidence to find him guilty of intentional unauthorized access.

Phillips makes a subsidiary argument that because the TXClass website was a public application, he, like any internet user, was a *de facto* authorized user. In essence, Phillips contends that his theft of other people's data from TXClass merely exceeded the preexisting generic authorization that he maintained as a user of the World Wide Web, and he cannot be considered an unauthorized user under § 1030(a)(5)(A)(ii).

This argument misconstrues the nature of obtaining "access" to an internet application and the CFAA's use of the term "authorization." While it is true that any internet user can insert the appropriate URL into a web browser and thereby view the "TXClass Administrative Training System" log-in web page, a user cannot gain access to the TXClass application itself without a valid Social Security

number password to which UT has affirmatively granted authorization.[4] Neither Phillips, nor members of the public, obtain such authorization from UT merely by viewing a log-in page, or clicking a hypertext link. Instead, courts have recognized that authorized access typically arises only out of a contractual or agency relationship.[5] While Phillips was authorized to use his UT email account and engage in other activities defined by UT's acceptable

---

[4] Phillips's contention that an individual's ability to view TXClass's log-in webpage amounts to a general grant of authorized access to the public-at-large is unsupported by various judicial interpretations of what constitutes obtaining access to a protected computer. *See, e.g., State v. Allen,* 260 Kan. 107, 917 P.2d 848 (1996) (under Kansas computer crime statute, until a computer user proceeds beyond introductory banners and log-in screens by use of a password, he has not accessed the program); *State v. Riley,* 121 Wash.2d 22, 846 P.2d 1365 (1993) (en banc) (attempted entry into computer using randomly generated passwords is not access until a successful password is found allowing entry); *see also Role Models, Inc. v. Jones,* 305 F.Supp.2d 564 (D.Md.2004) (mere receipt of information from a protected computer is not equivalent to obtaining access under CFAA).

[5] *See, e.g., Int'l Airport Ctrs. LLC v. Citrin,* 440 F.3d 418 (7th Cir.2006) (authorized access to company computer terminated when employee violated employment contract); *EF Cultural Travel BV v. Explorica, Inc.,* 274 F.3d 577 (1st Cir.2001) (confidentiality agreement defined authorized access to travel company's computerized pricing information); *United States v. Czubinski,* 106 F.3d 1069 (1st Cir.1997) (employer assignment of a confidential password created authorization); *Pac. Aerospace & Elecs., Inc. v. Taylor,* 295 F.Supp.2d 1188 (E.D.Wash.2003) (former employees' unauthorized access in violation of confidentiality and employment agreements merited imposition of preliminary injunction); *Shurgard Storage Ctrs., Inc. v. Safeguard Self-Storage, Inc.,* 119 F.Supp.2d 1121 (W.D.Wash.2000) (employees not authorized to obtain proprietary information from former employer because agency relationship had terminated); *YourNetDating, Inc. v. Mitchell,* 88 F.Supp.2d 870 (N.D.Ill.2000) (programmer's hacking of former employer's dating service website that redirected users to a pornographic website was unauthorized access and merited temporary restraining order).

computer use policy, he was never authorized to access TXClass. The method of access he used makes this fact even more plain. In short, the government produced sufficient evidence at trial to support Phillips's conviction under § 1030(a)(5)(A)(ii).

B. Constructive Amendment of the Indictment

For the first time on appeal, Phillips alleges as error that the district court constructively amended his indictment in its jury instructions. The district court charged the jury based on the Government's proposed instruction and a modified version of the Eleventh Circuit's Criminal Pattern Jury Instruction 42.3 that adopts language from §§ 1030(a)(5)(A)(i) and (B)(i). Subsection (i) punishes an individual who "knowingly causes the transmission of a program . . . to a protected computer." Phillips was indicted, however, not for *knowingly transmitting a program* under § 1030(a)(5)(A)(i), but for *intentionally accessing a protected computer* under § 1030(a)(5)(A)(ii). As Phillips did not object to the instruction at trial, we review this disparity between the indictment and jury charge for plain error. *United States v. Bieganowski,* 313 F.3d 264, 287 (5th Cir.2002) (constructive amendment claims raised for the first time on appeal reviewed for plain error).

Phillips asserts that the deviation between the terms of the charged offense and the language of the jury instruction was plain and adversely affected his substantial rights in two ways. First, the jury instruction impermissibly reduced the Government's burden of proof by not requiring the jury to find that he intentionally accessed TXClass without authorization, but instead only that he transmitted a program without authorization. Second,

Phillips claims that while § 1030(a)(5)(A)(ii) requires the Government to prove that he "intentionally" accessed a protected computer without authorization, the instruction required the jury to find only that Phillips "knowingly" caused the transmission of a program, not that he knowingly did so without authorization. Put otherwise, Phillips argues that since § 1030(a)(5)(A)(ii)'s scienter element applies to both the phrase "causes the transmission" and "without authorization," the district court erred in submitting an instruction in which the scienter element applied only to the act of transmitting a program.

Constructive amendment of an indictment occurs when the trial court "through its instructions and facts it permits in evidence, allows proof of an essential element of the crime on an alternative basis provided by the statute but not charged in the indictment." *United States v. Slovacek,* 867 F.2d 842, 847 (5th Cir.), *cert. denied,* 490 U.S. 1094, 109 S.Ct. 2441, 104 L.Ed.2d 997 (1989) (citing *Stirone v. United States,* 361 U.S. 212, 215-19, 80 S.Ct. 270, 272-74, 4 L.Ed.2d 252 (1960)). In evaluating whether constructive amendment has occurred, we consider "whether the jury instruction, taken as a whole, is a correct statement of the law and whether it clearly instructs jurors as to the principles of law applicable to the factual issues confronting them." *United States v. Guidry,* 406 F.3d 314, 321 (5th Cir.2005) (internal quotation marks omitted).

With respect to Phillips's first argument, the district court's instruction plainly modified an essential element of the charged offense by supporting the act of accessing a protected computer under subsection (ii) on the basis of transmitting a program under subsection (i). *See, e.g., United States v. Reyes,* 102 F.3d 1361 (5th Cir.1996) (jury

instruction permitting conviction based on proof of conspiracy to possess with the intent to distribute marijuana constructively amended indictment that charged not conspiracy, but the substantive offense itself). This was a classic constructive amendment. Why the Government overlooked the inconsistency between the statutory provision cited in the indictment and the provision described in the jury charge is a mystery.

We nonetheless find no reversible plain error with respect to the transmission/access discrepancy. Phillips gained access to TXClass by the act of transmitting the brute-force attack program. The factual predicates for Phillips's particular conviction under the jury charge and the indictment – knowingly transmitting a program and intentionally accessing a protected computer – are identical. There is no conceivable basis upon which the jury could have concluded that Phillips transmitted the program and obtained information from UT's database without having also accessed a protected computer. The instruction on this element of the charged offense, although incorrect, was immaterial.

Phillips's second argument is that the indictment charged him with "intentionally access[ing] a protected computer without authorization," while the jury instruction only required that he "knowingly" transmitted the program.

We agree that the plain language of the statute, tracked in the indictment, indicates that the actus reus was the *intentional* unauthorized access of a protected computer. In fact, the 1986 amendment to § 1030(a)(5) changed the scienter requirement from "knowingly" to "intentionally" because of Congress's concern that the

"knowingly" standard "might be inappropriate for cases involving computer technology."[6] *See* S.Rep. No. 99-432, at 5, *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2483 (1986); *Morris,* 928 F.2d at 507.[7]

The district court instructed the jury that to convict, it must find that Phillips "knowingly caused the transmission of a program" and that he "so acted without the authorization" of appropriate persons or entities. This instruction, as Phillips contends, does not fully convey that the jury must find that Phillips intentionally acted without authorization. However, as discussed above in the context of his sufficiency claim, the evidence leaves no doubt that Phillips knew he was unauthorized to transmit an invasive computer program designed to gain access to the TXClass system and to steal thousands of Social Security numbers. It beggars belief that, having transmitted such a program, Phillips did not intend to access a protected computer and that he [sic] access be unauthorized.[8] To the extent the jury instructions were wrong, the

---

[6] Discussion of the changes to the scienter elements of § 1030 in the Senate report focused on § 1030(a)(2), but the same alteration of "knowingly" to "intentionally" was made to § 1030(a)(5)(A)(ii) and the report explicitly states that "[t]he 'intentional' standard [in new subsection § 1030(a)(5)] is the same as that employed in Section 2(a)(1) and 2(b)(1) of the bill." S.Rep. No. 99-432, at 10 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2488 (1986).

[7] *Compare* §§ 1030(a)(5)(A)(i) and (ii), *with* § 1030(a)(1), which criminalizes the act of knowingly "exceed[ing] authorized access," without a requirement of intentional conduct.

[8] We note that, in any event, the district court rectified its error in misstating the scienter requirement as applied to Phillips's access. The court instructed the jury that "knowingly" means "that the act was done voluntarily and intentionally, not because of mistake or accident."

errors did not affect Phillips's substantial rights. *See Bieganowski, supra.*

C. Lesser-Included Offense Instruction

Phillips next contends that the district court improperly failed to instruct the jury on a lesser-included offense under § 1030(a)(5)(A)(iii), which is a misdemeanor.[9] Phillips's counsel actually raised this issue at trial, and the judge invited him to submit relevant authority, but he did not pursue the claim further or submit a proposed charge, and he failed to object to the jury charge. That defense counsel remained aware of the distinction between the mens rea requirements in the charged offense and the lower standard of conduct and damage betokened in the misdemeanor offense is clear from his closing argument; he observed that Phillips must be shown to have acted "recklessly" rather than with negligence.

---

[9] Section 1030(a)(5)(A)(ii) applies to whoever "intentionally accesses a protected computer without authorization, and as a result of such conduct recklessly causes damage. . . ." In contrast, § 1030(a)(5)(A)(iii) does not contain a scienter element with respect to causing damage following unauthorized access, but applies to anyone who "intentionally accesses a protected computer without authorization, and as the result of such conduct, causes damage" irrespective of mens rea and of any minimum damage requirement.

The differing degrees of culpability envisioned by Congress for the two subsections are reflected in the punishments Congress allotted to their violation. According to § 1030(c)(2)(A), violation of subsection (a)(5)(A)(iii), i.e., intentional unauthorized access and subsequent damage however caused, is a Class A misdemeanor punishable by a fine or imprisonment not exceeding one year, or both. *See* 18 U.S.C. § 3559(a)(6). Subsection (a)(5)(A)(ii), however, is a Class E felony, *see* 18 U.S.C. § 3559(a)(5), punishable by fine, imprisonment not exceeding five years, or both. § 1030(c)(4)(B).

We construe this train of events as a waiver of the argument Phillips now urges. Waiver is an "affirmative choice by the defendant to forego any remedy available to him, presumably for real or perceived benefits." *United States v. Dodson,* 288 F.3d 153, 160 (5th Cir.2002); *see also United States v. Olano,* 507 U.S. 725, 113 S.Ct. 1770, 123 L.Ed.2d 508 (1993) (waiver is the intentional relinquishment of a known right). The known right here was the at least arguable right to obtain a lesser-included offense instruction for a misdemeanor. The perceived benefit lay in counsel's strategic decision to pursue full acquittal if he could persuade the jury that Phillips hadn't recklessly caused damage. The judicial system can self-correct only if counsel voices an objection clearly at the proper time in the proceedings. Dropping hints as to a trial court's error, and awaiting the trial outcome to pursue the objection further, is inconsistent with counsel's duty of candor and clarity. This objection was waived. *See United States v. Salerno,* 108 F.3d 730, 740 (7th Cir.1997) (defendant's "lack of request for such an instruction coupled with his affirmative acceptance of the court's final jury instructions demonstrates that he intentionally relinquished his known right").

D. Restitution Award

Finally, Phillips contends that the district court erred in its award of restitution for costs incurred by UT in conducting a computer damage and systems evaluation and contacting individuals whose biographical information and Social Security numbers were stolen. Since Phillips raises this issue for the first time on appeal, we review the award for plain error. *United States v. Garza,* 429 F.3d 165, 169 (5th Cir.2005). There is no error at all.

A defendant sentenced under provisions of the Mandatory Restitution to Victims Act ("MRVA"), 18 U.S.C. § 3663A, is responsible for providing restitution only to victims who were directly and proximately harmed by the conduct underlying the offense for which he was convicted. *See* 18 U.S.C. § 3663A(a)(2); *United States v. Griffin,* 324 F.3d 330, 368 (5th Cir.2003). The MRVA applies to cases in which an identifiable victim has suffered "pecuniary loss," *see* 18 U.S.C. § 3663A(c)(1)(B), and expressly permits reimbursement of victims for "expenses incurred during participation in the investigation or prosecution" of the predicate offense. *See* § 3663A(b)(4).

Relying on *United States v. Schinnell,* 80 F.3d 1064 (5th Cir.1996), Phillips asserts that restitution of money spent by UT in contacting the victims of his electronic intrusions is barred by § 3663A(b)(1), a provision that precludes an award of "consequential damages." *Schinnell,* 80 F.3d at 1070-71;[10] *see also United States v. Onyiego,* 286 F.3d 249, 256 (5th Cir.2002) (district court award of restitution for legal fees victim incurred in defending collection actions caused by defendant's crime barred by § 3663A(b)(1)).

Schinnell's reasoning is inapplicable to the instant case. First, *Schinnell* involved a separate restitutionary provision, while § 3663A(b)(4), applicable here, explicitly

---

[10] Section 3663A(b)(1) applies to "offense[s] resulting in damage to or loss or destruction of property" and limits restitution to either the return of the property, or if return is impossible, impracticable, or inadequate, to the greater of the value of the property on the date of the loss or its value at sentencing. *Schinnell* involved interpretation of § 3663(b)(1) of the Victim and Witness Protection Act, 18 U.S.C. § 3663, which is identical to the MRVA's § 3663A(b)(1). *See Schinnell,* 80 F.3d at 1070.

authorizes restitution of expenses "incurred during participation in the investigation or prosecution of the offense." UT was a victim, and it collaborated with the investigation and incurred costs to notify other victims of Phillips's data theft in order to determine whether they had suffered further damage.

Second, *Schinnell* involved a violation of § 1343, the federal wire fraud statute, not § 1030(a)(5)(ii). The CFAA, unlike § 1343, precisely defines the nature of the loss resulting from unauthorized access of a protected computer that Congress sought to remedy:

> [T]he term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service. . . .

§ 1030(e)(11); *see also* S.Rep. No. 99-432, at 11, *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2488-89 (1986). *Schinnell* is based on a wholly distinguishable statutory framework.

III. CONCLUSION

For the foregoing reasons, the conviction and sentence are AFFIRMED.

UNITED STATES DISTRICT COURT
Western District of Texas
AUSTIN DIVISION

UNITED STATES OF AMERICA

v.

CHRISTOPHER ANDREW PHILLIPS

Defendant.

Case Number A-04-CR-247(1)-LY
USM Number 28937-180

JUDGMENT IN A CRIMINAL CASE
(For Offenses Committed On or After November 1, 1987)

(Filed Sep. 15, 2005)

The defendant, **CHRISTOPHER ANDREW PHILLIPS**, was represented by Allan Williams and Steve Brittain.

The defendant was found guilty on Count(s) 1 of the Indictment (and not guilty on Count(s) 2 and 3) by a jury verdict on June 10, 2005 after a plea of not guilty. Accordingly, the defendant is adjudged guilty of such Count(s), involving the following offense(s):

Title & Section	Nature of Offense	Date Offense Concluded	Count Number(s)
18:1030(a)(5)(A)(ii)	FRAUD AND RELATED ACTIVITIES IN CONNECTION WITH COMPUTERS	03/02/2003	1

As pronounced on **SEPTEMBER 6, 2005**, the defendant is sentenced as provided in pages 2 through 5 of this Judgment. The sentence is imposed pursuant to the Sentencing Reform Act of 1984.

It is further ordered that the defendant shall notify the United States Attorney for this district within 30 days of any change of name, residence, or mailing address until all fines, restitution, costs and special assessments imposed by this Judgment are fully paid. If ordered to pay restitution, the defendant shall notify the Court and United States Attorney of any material change in the defendant's economic circumstances.

Signed this the 15th day of September, 2005.

/s/ Lee Yeakel
LEE YEAKEL
United States District Judge

PROBATION

The defendant is hereby placed on probation for a term of FIVE (5) YEARS.

While on probation, the defendant shall comply with the mandatory, standard and if applicable, the special conditions that have been adopted by this Court as set forth in pages 3 and 4 of this judgment; and shall comply with the following additional conditions:

X The defendant shall, upon request of the United States Probation Office, authorize release of any and all financial information, to include income records, income tax records, and social security records, by

execution of a release of financial information form or by other appropriate means.

X The defendant shall not utilize the Internet services on the computer, unless for monitored work related business and/or educational purposes, or other uses by the probation officer.

X Unless otherwise authorized by the probation officer, the defendant shall not utilize a computer, which utilizes a modem or which is otherwise connected to the Internet, unless for monitored business and/or educational purposes. The defendant shall permit the United States Probation Officer to monitor the computer for possible violations, knowing the monitoring may include the use of special hardware/software programs or the utilization of a designated Internet Service Provider, at the defendant's own expense.

X The defendant shall not subscribe to any computer online service, nor shall the defendant access any Internet service during the length of his supervision, unless approved in advance in writing by the United States Probation Officer. The defendant may not possess Internet capable software on any hard drive, disk, floppy disk, compact disk, DVD, diskette, magnetic tape, or any other electronic storage media, unless specifically approved in advance in writing by the United States Probation Officer.

CONDITIONS OF PROBATION

Mandatory Conditions:

1) The defendant shall not commit another federal, state, or local crime.

2) The defendant shall not unlawfully possess a controlled substance. The defendant shall refrain from any unlawful use of a controlled substance. The defendant shall submit to one drug test within 15 days of release from imprisonment and at least two periodic drug tests thereafter, as determined by the court.

3) In supervised release cases only, the defendant must report to the probation office in the district to which the defendant is released within 72 hours of release from custody of the Bureau of Prisons.

4) If convicted of a felony, the defendant shall not possess a firearm, ammunition, destructive device, or any other dangerous weapon.

5) The defendant shall cooperate in the collection of DNA as directed by the probation officer if the collection of such a sample is authorized pursuant to section 3 of the DNA Analysis Backlog Elimination Act of 2000 (42 U.S.C. § 1413a).

6) If convicted of a sexual offense as described in 18 U.S.C. § 4042(c)(4), the defendant shall register with the state sex offender registration agency in the state where the defendant resides, works, or is a student, as directed by the probation officer.

7) If convicted of a domestic violence crime as defined in 18 U.S.C. § 3561(b), the defendant shall participate in an approved program for domestic violence.

8) If the judgment imposes a fine or restitution, it is a condition of supervision that the defendant pay in accordance with the Schedule of Payments sheet of the judgment.

Standard Conditions:

1) the defendant shall not leave the judicial district without the permission of the court or probation officer.

2) The defendant shall report to the Probation Officer and shall submit a truthful and complete written report within the first five days of each month.

3) The defendant shall answer truthfully all inquires by the Probation Officer and follow the instructions of the Probation Officer.

4) The defendant shall support his or her dependents and meet other family responsibilities.

5) The defendant shall work regularly at a lawful occupation, unless excused by the Probation Officer for schooling, training, or other acceptable reasons.

6) The defendant shall notify the Probation Officer at least ten days prior to any change in residence or employment.

7) The defendant shall refrain from excessive use of alcohol and shall not purchase, possess, use, distribute, or administer any controlled substance or any paraphernalia related to any controlled substances, except as prescribed by a physician.

8) The defendant shall not frequent places where controlled substances are illegally sold, used, distributed, or administered.

9) The defendant shall not associate with any persons engaged in criminal activity, and shall not associate with any person convicted of a felony unless granted permission to do so by the Probation Officer.

10) The defendant shall permit a Probation Officer to visit him or her at any time at home or elsewhere and

shall permit confiscation of any contraband observed in plain view by the Probation Officer.

11) The defendant shall notify the Probation Officer within seventy-two hours of being arrested or questioned by a law enforcement officer.

12) The defendant shall not enter into any agreement to act as an informer or a special agent of a law enforcement agency without the permission of the Court.

13) As directed by the probation officer, the defendant shall notify third parties of risks that may be occasioned by the defendant's criminal record or personal history or characteristics, and shall permit the probation officer to make such notifications and to confirm the defendant's compliance with such notification requirement.

14) If convicted of a sexual offense as described in 18 U.S.C. § 4042(c)(4), or has a prior conviction of a State or local offense that would have been an offense as described in 18 U.S.C. § 4042(c)(4) if a circumstance giving rise to Federal jurisdiction had existed, the defendant shall participate in a sex offender treatment program approved by the probation officer. The defendant shall abide by all program rules, requirements and conditions of the sex offender treatment program, including submission to polygraph testing, to determine if the defendant is in compliance with the conditions of release. The defendant may be required to contribute to the cost of the services rendered (copayment) in an amount to be determined by the probation officer, based on the defendant's ability to pay.

15) The defendant shall submit to an evaluation for substance abuse or dependency treatment as directed by the probation officer, and if deemed necessary by

the probation officer, the defendant shall participate in a program approved by the probation officer for treatment of narcotic addiction or drug or alcohol dependency which may include testing and examination to determine if the defendant has reverted to the use of drugs or alcohol. The defendant may be required to contribute to the cost of the services rendered (copayment) in an amount to be determined by the probation officer, based upon the defendant's ability to pay.

16) The defendant shall submit to an evaluation for mental health counseling as directed by the probation officer, and if deemed necessary by the probation officer, the defendant shall participate in a mental health program approved by the probation officer. The defendant may be required to contribute to the cost of the services rendered (copayment) in an amount to be determined by the probation officer, based upon the defendant's ability to pay.

17) If the defendant is excluded, deported, or removed upon release from imprisonment, the term of supervised release shall be a non-reporting term of supervised release. The defendant shall not illegally re-enter the United States. If the defendant lawfully re-enters the United States during the term of supervised release, the defendant shall immediately report in person to the nearest U.S. Probation Office.

18) If the judgment imposes other criminal monetary penalties, it is a condition of supervision that the defendant pay such penalties in accordance with the Schedule of Payments sheet of the judgment.

19) If the judgment imposes a fine, special assessment, restitution, or other criminal monetary penalties, it is a condition of supervision that the defendant shall

provide the probation officer access to any requested financial information.

20) If the judgment imposes a fine, special assessment, restitution, or other criminal monetary penalties, it is a condition of supervision that the defendant shall not incur any new credit charges or open additional lines of credit without the approval of the probation officer unless the defendant is in compliance with the payment schedule.

The Court further adopts such of the following special conditions applied to the supervised person by the judge at the time of sentencing:

1) **COMMUNITY CONFINEMENT:** The defendant shall reside in a Community Corrections Center for a period of ___ months to commence on ___. Further, once employed, the defendant shall pay 25% of his/her weekly gross income for his/her subsistence as long as that amount does not exceed the daily contract rate.

2) **HOME DETENTION:** The defendant shall participate in the Home Confinement Program for a period of ___ days/months. During this time the defendant shall remain at his/her place of residence except for employment and other activities approved in advance by the probation officer. The defendant shall maintain a telephone at his/her place of residence without "call forwarding," a "modem," "caller ID," "call waiting," or portable cordless telephones for the above period. At the direction of the probation officer, the defendant shall wear an electronic monitoring device and follow electronic monitoring procedures specified by the probation officer. The court further orders that the defendant shall pay for the costs of Home Confinement, as directed by the probation officer.

3) **COMMUNITY SERVICE:** The defendant shall perform 500 hours of community service work under the direction and supervision of the probation officer, to be completed during the period of probation.

CRIMINAL MONETARY PENALTIES/SCHEDULE

The defendant shall pay the following total criminal monetary penalties in accordance with the schedule of payments set forth. Criminal Monetary Penalties, except those payments made through Federal Bureau of Prisons' Inmate Financial Responsibility Program shall be paid through the Clerk, United States District Court, 200 W. 8th Street, Room 130 Austin, Texas 78701.

	Assessment	Fine	Restitution
TOTAL:	$100.00	$0	$170,056.00

Special Assessment

It is ordered that the defendant shall pay to the United States a special assessment of $100.00. Payment of this sum shall begin immediately.

Fine

The fine is waived because of the defendant's inability to pay.

Restitution

The defendant shall pay restitution in the amount of $170,056.00 through the Clerk, U.S. District Court, for distribution to the payee(s). Payment of this sum shall begin immediately. The Court determines that the defendant

does not have the ability to pay interest and therefore waives the interest requirement pursuant to 18 U.S.C. § 3612(f)(3).

Name of Payee	Amount of Restitution
THE UNIVERSITY OF TEXAS AT AUSTIN Attention: L. B. Brady Information Technology Services P. O. Box 7404 Austin, TX 78713-7407 (512) 232-9610 Reference Number: 18-2300-0095	$170,056.00

If the defendant makes a partial payment, each payee shall receive an approximately proportioned payment, unless specified otherwise in the priority order or percentage payment column below. However, pursuant to 18 U.S.C. § 3664(i), all non-federal victims must be paid before the United States is paid.

If the fine is not paid, the court may sentence the defendant to any sentence which might have been originally imposed. See 18 U.S.C. §3614.

The defendant shall pay interest on any fine or restitution of more than $2,500.00, unless the fine or restitution is paid in full before the fifteenth day after the date of the judgment, pursuant to 18 U.S.C. §3612(f). all payment options may be subject to penalties for delinquency and default, pursuant to 18 U.S.C. §3612(g).

Payments shall be applied in the following order: (1) assessment, (2) restitution principal, (3) restitution interest, (4) fine principal, (5) community restitution, (6) fine

interest (7) penalties, and (8) costs, including cost of prosecution and court costs.

Findings for the total amount of losses are required under Chapters 109A, 110, 110A, and 113A of Title 18 for offenses committed on or after September 13, 1994, but before April 23, 1996.

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

No. 05-51271

UNITED STATES OF AMERICA

Plaintiff-Appellee

v.

CHRISTOPHER ANDREW PHILLIPS

Defendant-Appellant

Appeal from the United States District Court
for the Western District of Texas, Austin

ON PETITION FOR REHEARING EN BANC

(Opinion 1/24/07, 5 Cir., ___, ___ F.3d ___)

(Filed March 1, 2007)

Before JONES, SMITH, and STEWART, Circuit Judges.

PER CURIAM:

(X) The petition for en banc rehearing is out of time. The court has allowed the filing of the late petition for en banc rehearing. Treating the Petition for Rehearing En Banc as a Petition for Panel Rehearing, the Petition for Panel Rehearing is DENIED. No member of the panel nor judge in regular active service of the court having requested that the court be polled on Rehearing En Banc (FED. R. APP. P.

and 5th CIR. R. 35), the Petition for Rehearing En Banc is DENIED.

( ) The petition for en banc rehearing is out of time. The court has allowed the filing of the late petition for en banc rehearing. Treating the Petition for Rehearing En Banc as a Petition for Panel Rehearing, the Petition for Panel Rehearing is DENIED. The court having been polled at the request of one of the members of the court and a majority of the judges who are in regular active service and not disqualified not having voted in favor (Fed. R. App. P. and 5th Cir. R. 35), the Petition for Rehearing En Banc is DENIED.

ENTERED FOR THE COURT:

/s/ Edith K. Jones
United States Circuit
Judge

No. 06-1602

In the Supreme Court of the United States

CHRISTOPHER ANDREW PHILLIPS, PETITIONER

v.

UNITED STATES OF AMERICA

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FIFTH CIRCUIT

BRIEF FOR THE UNITED STATES IN OPPOSITION

PAUL D. CLEMENT
Solicitor General
Counsel of Record

ALICE S. FISHER
Assistant Attorney General

MICHAEL A. ROTKER
Attorney

Department of Justice
Washington, D.C. 20530-0001
(202) 514-2217

QUESTION PRESENTED

Whether the district court committed reversible plain error by instructing the jury that it could convict petitioner for knowingly transmitting a program to a protected computer, in violation of 18 U.S.C. 1030(a)(5)(A)(i) (Supp. IV 2004), where the indictment charged that petitioner intentionally accessed a protected computer without authorization, in violation of 18 U.S.C. 1030(a)(5)(A)(ii) (Supp. IV 2004).

TABLE OF CONTENTS

Page

Opinion below 1
Jurisdiction 1
Statement 1
Argument 8
Conclusion 15

TABLE OF AUTHORITIES

Cases:

Almendarez-Torres v. *United States*, 523 U.S. 224 (1998) 9
Chapman v. *California*, 386 U.S. 18 (1967) 11
Hamling v. *United States*, 418 U.S. 87 (1974) 10
Johnson v. *United States*, 520 U.S. 461 (1997) 7, 9, 13, 14
Murphy v. *United States*, 546 U.S. 1097 (2006) 9
Neder v. *United States*, 527 U.S. 1 (1999) 11
Stirone v. *United States*, 361 U.S. 212 (1960) 10, 11
United States v. *Brown*, 400 F.3d 1242 (10th Cir. 2005) 14
United States v. *Cotton*:
535 U.S. 625 (2002) 9, 12, 13, 14
261 F.3d 397 (4th Cir. 2001), rev'd, 535 U.S. 625 (2002) 12, 13
United States v. *Floresca*, 38 F.3d 706 (4th Cir. 1994) 12, 13
United States v. *Miller*, 471 U.S. 130 (1985) 9

Cases—Continued: Page

United States v. *Murphy*, 406 F.3d 857 (7th Cir. 2005), cert. denied, 546 U.S. 1097 (2006) 13
United States v. *Thomas*, 274 F.3d 655 (2d Cir. 2001) ... 12

Constitution and statutes:

U.S. Const.:
Art. I, § 10, Cl. 1 (Ex Post Facto Clause) 6
Amend. V (Grand Jury Clause) 9
18 U.S.C. 1028(a)(6) (Supp. IV 2004) 4
18 U.S.C. 1029(a)(3) 4
18 U.S.C. 1030(a)(5) (2000 & Supp. IV 2004) 6, 8
18 U.S.C. 1030(a)(5)(A)(i) (Supp. IV 2004) 6, 10
18 U.S.C. 1030(a)(5)(A)(ii) (Supp. IV 2004) 1, 4, 6, 7, 8, 10

Miscellaneous:

11th Cir. Pattern Jury Instructions–Criminal Cases (2003) 6
4 Wayne R. LaFave et al., *Criminal Procedure* (2d ed. 1999) 10, 11

In the Supreme Court of the United States

No. 06-1602

CHRISTOPHER ANDREW PHILLIPS, PETITIONER

v.

UNITED STATES OF AMERICA

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FIFTH CIRCUIT

BRIEF FOR THE UNITED STATES IN OPPOSITION

OPINION BELOW

The opinion of the court of appeals (Pet. App. 1-17) is reported at 477 F.3d 215.

JURISDICTION

The judgment of the court of appeals was entered on January 24, 2007. A petition for rehearing was denied on March 1, 2007 (Pet. App. 29-30). The petition for a writ of certiorari was filed on May 30, 2007. The jurisdiction of this Court is invoked under 28 U.S.C. 1254(1).

STATEMENT

Following a jury trial in the United States District Court for the Western District of Texas, petitioner was convicted of intentionally accessing a protected computer without authorization and recklessly causing damage, in violation of 18 U.S.C. 1030(a)(5)(A)(ii) (Supp. IV

2004). He was sentenced to five years of probation, five hundred hours of community service, and restitution of $170,056. Pet. App. 19, 26. The court of appeals affirmed. *Id.* at 1-17.

1. Petitioner became a student at the University of Texas at Austin (UT) in 2001. Despite signing UT's "acceptable use" computer policy, in which he agreed not to perform port scans using his university computer account,[1] petitioner used various programs designed to scan computer networks and steal encrypted data and passwords. He broke into hundreds of computers, including machines belonging to other UT students, private businesses, United States Government agencies, and the British Armed Services webserver. Petitioner thereby obtained a substantial amount of personal and proprietary data, such as credit card numbers, bank account information, student financial aid statements, birth records, passwords, and Social Security numbers. Pet. App. 2; Gov't C.A. Br. 4-5.

Petitioner's port scanning was detected by UT's Information Security Office (ISO), which warned him on three separate occasions to stop trying to breach the security of computer systems. Despite those warnings, petitioner continued to scan and infiltrate computers inside and outside the UT system, adding to his data-

[1] "Port scanning is a technique used by computer hackers by which an individual sends requests via a worm or other program to various networked computer ports in an effort to ascertain whether particular machines have vulnerabilities that would leave them susceptible to external intrusion. Often used as an initial step in launching an attack on another computer or transmitting a virus, port scanning is a relatively unsophisticated, but highly effective, reconnaissance method, likened at trial by UT's information technology chief as the electronic equivalent of 'rattling doorknobs' to see if easy access can be gained to a room." Pet. App. 2 n.1.

base of stolen information. Pet. App. 2-3; Gov't C.A. Br. 5-6.

In early 2002, petitioner designed a "brute force attack" program[2] to breach the UT computer system via a portal known as the "TXClass Learning Central: A Complete Training Resource for UT Faculty and Staff." TXClass was used by UT faculty and staff as a resource for continuing professional education of UT employees. Non-employee students such as petitioner were not authorized to use TXClass. Authorized users gained access to their TXClass accounts by typing their Social Security numbers in a field on the TXClass website's log-on page. Petitioner's "brute-force attack" program was designed to exploit the log-on protocol, automatically transmitting to the website as many as six Social Security numbers per second, at least some of which would correspond to those of authorized TXClass users. When the program hit a valid Social Security number in the TXClass database, it extracted personal information corresponding to that number and provided petitioner a "back door" into a larger UT database containing information about current and prospective UT students, employment applicants, and charitable donors. Over a fourteen-month period, petitioner obtained data on more than 45,000 current and prospective students, donors, and alumni. Pet. App. 3-4; Gov't C.A. Br. 7-8.

Petitioner's actions adversely affected the UT computer system, requiring UT to spend more than $122,000 to assess the damage and $60,000 to notify victims that their personal information and Social Security numbers

---

[2] "'Brute-force attack' is term of art in computer science used to describe a program designed to decode encrypted data by generating a large number of passwords." Pet. App. 3 n.2.

had been illegally obtained. Pet. App. 4; Gov't C.A. Br. 11.

UT contacted the Secret Service, and the ensuing investigation led to petitioner. Thereafter, petitioner admitted that he had created the brute-force attack program to obtain personal information from the UT system, but he disavowed that he intended to use or sell it. Pet. App. 4; Gov't C.A. Br. 10.

2. A federal grand jury in the Western District of Texas returned a four-count indictment charging petitioner with intentionally accessing a protected computer without authorization and recklessly causing damage, in violation of 18 U.S.C. 1030(a)(5)(A)(ii) (Supp. IV 2004) (Count 1), fraud in connection with access devices, in violation of 18 U.S.C. 1029(a)(3) (Counts 2 and 3), and fraud in connection with authentication features, in violation of 18 U.S.C. 1028(a)(6) (Supp. IV 2004) (Count 4). Pet. App. 4; Gov't C.A. Br. 3. Petitioner was tried before a jury. Pet. App. 4. At the close of the evidence, the district court provided the jury with the following instruction concerning Count 1:

> Title 18, United States Code, Section 1030(a)(5) makes it a Federal crime or offense for anyone, through means of a computer used in interstate commerce or communications, to knowingly and without authorization, cause the transmission of any program, code or command to another computer or computer system and recklessly causes damage to [the] receiving computer, computer system, network, information, data or program, or withhold or deny, or cause the withholding or denial, of the use of a computer, computer services, system or network, information, data or program.

[Petitioner] can be found guilty of that offense only if all of the following facts are proved beyond a reasonable doubt:

First: That [petitioner], through means of a computer used in interstate commerce or communications, knowingly caused the transmission of a program, information, code or command to another computer or computer system, as charged;

Second: That [petitioner], by causing the transmission, acted with reckless disregard of a substantial and unjustifiable risk that the transmission would damage the receiving computer, computer system, information, data or program[,] or withhold or deny, or cause the withholding or denial, of the use of a computer, computer services, system or network, information, data or program;

Third: That [petitioner] so acted without the authorization of the persons or entities who own or are responsible for the computer system receiving the program, information, code or command; and

Fourth: That [petitioner's] acts caused loss or damage to one or more other persons of value aggregating $5,000 or more during any one year period.

Gov't C.A. Br. 25-26 (quoting charge).[3] Petitioner did not object to that instruction.

The jury convicted petitioner on Counts 1 and 4, and acquitted him on Counts 2 and 3. Petitioner timely filed a post-verdict motion for judgment of acquittal challenging the sufficiency of the evidence regarding the loss amount used to support his conviction on Count 1, and asserting that his conviction on Count 4 violated the Ex Post Facto Clause. Pet. App. 4-5. The district court denied the motion with respect to Count 1, but it granted the motion with respect to Count 4. *Id.* at 5 & n.3.

3. On appeal, petitioner contended, for the first time, that the jury instructions constructively amended the indictment by permitting the jury to convict him for violating Section 1030(a)(5)(A)(i)—*viz.*, knowingly causing the transmission of a program to a protected computer—when the indictment had only alleged a violation of Section 1030(a)(5)(A)(ii)—*viz.*, intentionally accessing a protected computer. Pet. App. 5-10. He further alleged that the deviation between the terms of the charged offense and the offense submitted to the jury warranted reversal of his conviction for two separate reasons. First, he alleged that the jury instruction failed to require the jury to find that he intentionally accessed TXClass without authorization, but instead only required that he transmitted a program without authorization. *Ibid.*; Pet. C.A. Br. 21. Second,

---

[3] As there was no pattern jury instruction for the Fifth Circuit with respect to this offense, the district court's charge was based on the government's proposed instruction, which was derived from the text of Section 1030(a)(5), 18 U.S.C. 1030(a)(5) (2000 & Supp. IV 2004), and a modified version of Eleventh Circuit Criminal Pattern Jury Offense Instruction 42.3 (2003). See Pet. App. 10; Gov't C.A. Br. 25.

he alleged that, while the charged offense, Section 1030(a)(5)(A)(ii), requires the government to prove that he "intentionally" accessed a protected computer without authorization, the jury instruction did not require the jury to find that he acted intentionally with respect to the lack of authorization. Pet. C.A. Br. 21-22. Petitioner conceded that he "did not object to the charge," *id.* at 20, and therefore that "[t]he standard of review is * * * plain error," *ibid.*, but he maintained that the asserted "constructive amendment" of the indictment qualified as reversible plain error, *id.* at 22-23.

The court of appeals affirmed. The court agreed with petitioner's concession that plain-error review applied because he failed to object below. Pet. App. 10. To prevail under that standard, petitioner must show that (1) there was error; (2) the error was plain; (3) the error affected his substantial rights; and (4) the error seriously affected the fairness, integrity, or public reputation of judicial proceedings. See *Johnson* v. *United States*, 520 U.S. 461, 466-467 (1997). Applying that standard to petitioner's first assertion, the court found that the jury instruction had plainly modified an essential element of the charged offense by "supporting the act of accessing a protected computer under subsection (ii) on the basis of transmitting a program under subsection (i)." Pet. App. 11. Nonetheless, the court found "no reversible plain error with respect to the transmission/access discrepancy" because there was "no conceivable basis upon which the jury could have concluded that [petitioner] transmitted the program and obtained information from UT's database without having also accessed a protected computer." *Id.* at 12. Accordingly, the instruction on that element of the offense, "although incorrect, was immaterial." *Ibid.*

The court of appeals also concluded that petitioner's second claim did not warrant reversal. The court agreed with petitioner that "the actus reus was the *intentional* unauthorized access of a protected computer." Pet. App. 12. But while the jury instruction did not explicitly require the jury to find "that [petitioner] intentionally acted without authorization," *id.* at 13, the court concluded that the evidence "leaves no doubt that [petitioner] knew he was unauthorized to transmit an invasive computer program designed to gain access to the TXClass system and to steal thousands of Social Security numbers," *ibid.* The court further explained: "It beggars belief that, having transmitted such a program, [petitioner] did not intend to access a protected computer and that he [sic] access be unauthorized." *Ibid.* Therefore, the court concluded that, "[t]o the extent the jury instructions were wrong, the errors did not affect [petitioner's] substantial rights." *Id.* at 13-14.[4]

ARGUMENT

Petitioner contends (Pet. 7-15) that the district court committed reversible plain error by instructing the jury concerning the "transmi[tting]" prong of 18 U.S.C. 1030(a)(5) (2000 & Supp. IV 2004) when the indictment alleged that petitioner had violated the "access[ing]"

---

[4] The court of appeals also rejected petitioner's argument, raised for the first time on appeal, that there was insufficient evidence that petitioner "intentionaly access[ed] a protected computer without authorization." Pet. App. 5 (quoting 18 U.S.C. 1030(a)(5)(A)(ii) (Supp. IV 2004)). After observing that petitioner was "never authorized to access TXClass," *id.* at 10, and that he "intentionally and meticulously executed both his intrusion into TXClass and the extraction of a sizable quantity of confidential personal data," *id.* at 8, the court concluded that "[t]here was no lack of evidence to find him guilty of intentional unauthorized access," *ibid.*

prong. Under the plain-error standard, a defendant is entitled to relief for an error to which he did not object at trial only if he can show that (1) there was error; (2) the error was plain; and (3) the error affected his substantial rights. If those three conditions are met, an appellate court may then exercise its discretion to notice a forfeited error, but only if the error (4) seriously affected the fairness, integrity, or public reputation of judicial proceedings. *Johnson* v. *United States*, 520 U.S. 461, 466-467 (1997); accord *United States* v. *Cotton*, 535 U.S. 625, 631-632 (2002). The court of appeals' conclusion that petitioner failed to satisfy the plain-error standard was correct, and petitioner identifies no circuit conflict on the application of that standard that warrants this Court's review. Indeed, this Court denied a petition for a writ of certiorari in another case raising a similar question concerning the application of the plain-error standard to constructive amendments, see *Murphy* v. *United States*, 546 U.S. 1097 (2006) (No. 05-6311),[5] and there is no reason for a different result in this case.

1. The Fifth Amendment's Grand Jury Clause states that "[n]o person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury." This Court has repeatedly held that the Grand Jury Clause requires that every element of a criminal offense be charged in a federal indictment. See, *e.g.*, *Almendarez-Torres* v. *United States*, 523 U.S. 224, 228 (1998); *United States* v. *Miller*,

---

[5] On June 20, 2007, the United States filed a brief in opposition to the petition for a writ of certiorari filed in *Pryor* v. *United States*, petition for cert. pending, No. 06-10280 (filed Mar. 23, 2007), which raises the same issue concerning the application of the plain-error standard to a constructive amendment claim.

471 U.S. 130, 136 (1985); *Hamling* v. *United States*, 418 U.S. 87, 117 (1974).

Petitioner contends (Pet. 6-15) that, by instructing the jury that it could convict if it found that the government had proven that petitioner knowingly transmitted a program, in violation of 18 U.S.C. 1030(a)(5)(A)(i), when the indictment alleged that petitioner had intentionally accessed a protected computer, in violation of 18 U.S.C. 1030(a)(5)(A)(ii), the district court permitted a "constructive amendment" of the indictment. See, *e.g.*, *Stirone* v. *United States*, 361 U.S. 212, 219 (1960) (reversing a verdict that may have rested on a factual theory different from that charged in the indictment on the ground that it was impossible to "know whether the grand jury would have included in its indictment a charge" based on that theory). Petitioner further contends that such a "constructive amendment" constitutes structural error, and thus automatically affects his substantial rights for purposes of the third prong of the plain-error standard. Pet. 6-10.

As a preliminary matter, not all deviations between the theory of guilt specified in the indictment and the government's evidence at trial constitute "constructive amendments." Where the divergence does not substantially alter the charged theory of guilt, lower courts have characterized it as a mere "variance" from the indictment, and have held that it affords no ground for reversal unless the divergence "is likely to have caused surprise or otherwise been prejudicial to the defense." 4 Wayne R. LaFave et al., *Criminal Procedure* § 19.6(c) at 808-809 & n.23 (2d ed. 1999) (citing cases). Only where the divergence sets an entirely new basis for conviction before the jury have lower courts characterized the divergence as a "constructive amendment" of the

indictment and generally held that it constitutes structural error (thereby requiring automatic reversal when an objection has been properly preserved). See *id.* § 19.6(c), at 811-812.

There is a substantial question whether the lower court decisions holding that a "constructive amendment" constitutes structural error remain valid in light of this Court's decisions holding that most constitutional errors are subject to harmless-error review. To the extent that lower courts have so held, cf. Pet. 8-10 (citing cases arising on plain-error review), those courts (like petitioner, see Pet. 6-10) have relied principally on this Court's decision in *Stirone*, which held that automatic reversal was warranted when the government proved an element at trial based on a factual theory that deviated from the factual theory advanced in the indictment and the defendant had raised a timely objection at trial. 361 U.S. at 217. *Stirone*, however, was decided before this Court held that harmless-error analysis was generally applicable to constitutional errors, see *Chapman* v. *California*, 386 U.S. 18, 22 (1967), and that harmless-error analysis was specifically applicable to the omission of an element of the offense from the jury's instructions, see *Neder* v. *United States*, 527 U.S. 1, 8-15 (1999).

2. Petitioner asserts (Pet. 10) that this Court's review is warranted to resolve a disagreement among the courts of appeals on whether errors of the sort at issue here constitute "structural errors" that necessarily affect petitioner's substantial rights for purposes of the third prong of the plain-error standard. Further review of that question is not warranted because, even if petitioner is correct that a constructive amendment is a structural error, he still would not be entitled to relief unless he could also satisfy the prerequisite for noticing

forfeited claims under the *fourth* prong of the plain-error standard: *i.e.*, by showing that the error seriously affected the fairness, integrity, or public reputation of judicial proceedings. Because petitioner cannot satisfy that prong, further review of the court of appeals' application of the third prong in this case is unwarranted.

Petitioner notes (Pet. 7-8) that, in *United States* v. *Floresca*, 38 F.3d 706 (1994) (en banc), the Fourth Circuit held that the "constructive amendment" of an indictment requires automatic reversal, even where an objection has not been properly preserved (and plain-error review is thus applicable). See *id.* at 714.[6] To the extent petitioner contends that this Court should adopt that rule, however, his contention is flawed. As petitioner tacitly recognizes (Pet. 11-13), *Floresca*'s reasoning has been called into question by this Court's intervening decision in *United States* v. *Cotton*, *supra*.

In *Cotton*, the district court sentenced the defendants to terms of imprisonment that exceeded the statutory maximum sentence that would have applied to the charge set out in the indictment. The Fourth Circuit reversed. *United States* v. *Cotton*, 261 F.3d 397, 404-407 (2001), rev'd, 535 U.S. 625 (2002). Relying on *Floresca*, it held that "sentencing a defendant for an unindicted crime" undermines the fairness, integrity, and public

---

[6] Although petitioner also (Pet. 6) cites *United States* v. *Thomas*, 274 F.3d 655 (2d Cir. 2001) (en banc), for the proposition that a "constructive amendment" automatically affects a defendant's substantial rights under the third prong of the plain-error test, the case—as petitioner himself recognizes (Pet. 7)—does not support the more ambitious proposition embraced by the Fourth Circuit, that a "constructive amendment" of an indictment *always* seriously affects the fairness, integrity, or public reputation of judicial proceedings (and thus requires automatic reversal even on plain-error review).

reputation of judicial proceedings in the same way that "convicting a defendant of an unindicted crime" does. *Id.* at 406 (emphasis omitted) (quoting *Floresca*, 38 F.3d at 714). This Court, however, reversed the court of appeals. It held that the defendants were not entitled to relief under the fourth prong of the plain-error standard because the evidence of the relevant sentence-enhancing fact that was not submitted to the jury (or charged in the indictment) was "overwhelming" and "essentially uncontroverted." *Cotton*, 535 U.S. at 633 (quoting *Johnson*, 520 U.S. at 470). The Court added that "[t]he real threat * * * to the 'fairness, integrity, and public reputation of judicial proceedings' would be if [the defendants], despite the overwhelming and uncontroverted evidence," were to receive a lesser sentence for a "less substantial" crime "because of an error that was never objected to at trial." *Id.* at 634.

In light of this Court's decision in *Cotton*, the Fourth Circuit's holding in *Floresca*—that the "constructive amendment" of an indictment requires automatic reversal even where an objection has not been properly preserved—should no longer be considered good law. The Fourth Circuit has not addressed the rule of *Floresca* since *Cotton*, and this Court has denied review in at least one case in which the petitioner alleged a circuit conflict with *Floresca*. See *United States* v. *Murphy*, 406 F.3d 857 (7th Cir. 2005), cert. denied, 546 U.S. 1097 (2006) (No. 05-6311). At a minimum, the Fourth Circuit should be permitted to reconsider the *Floresca* approach in an appropriate case before this Court intervenes. Indeed, as petitioner himself notes (Pet. 11-12), the Tenth Circuit has done precisely that and concluded that its pre-*Cotton* automatic reversal rule "no longer applies in a constructive amendment plain error case" in the wake of

Cotton. *United States* v. *Brown*, 400 F.3d 1242, 1253 n.6 (2005).

3. In the alternative, petitioner contends (Pet. 13-14) that, even if *Floresca* is no longer good law, the fourth prong of the plain-error standard is satisfied here because the evidence that he intentionally accessed the UT computer system without authorization was not "overwhelming" or "essentially uncontroverted." *Cotton*, 535 U.S. at 633 (quoting *Johnson*, 520 U.S. at 470). That fact-bound contention lacks merit and in any event does not warrant further review.

As the court of appeals concluded, the factual predicate for the transmission and access offenses—petitioner's use of the "brute-force attack program" to gain access to TXClass—was "identical," Pet. App. 12, and, therefore, there is "no conceivable basis upon which the jury could have concluded that [petitioner] transmitted the program and also obtained information from UT's database without having also accessed a protected computer." *Ibid.* Accordingly, while the district court erred in instructing the jury concerning transmission, the error was "immaterial," *ibid.*, because the jury's "transmission" finding necessarily included an "access" finding as well.[7] Moreover, the evidence that petitioner intentionally accessed TXClass without authorization was overwhelming. As the court of appeals observed, peti-

---

[7] Petitioner contends (Pet. 14) that he "did not 'transmit' any 'program.'" Regardless of whether he transmitted a "program," however, he clearly used the "brute-force attack program" to transmit social security numbers to the TXClass website in order to gain access to UT's database and extract information. The jury instructions permitted a finding of guilt based on the transmission not only of programs, but also of "information, code or command." See p. 5, *supra*. The social security numbers were "information" that petitioner transmitted.

tioner's "brute-force attack program was not an intended use of the UT network within the understanding of any reasonable computer user." *Id.* at 8. To the contrary, petitioner "intentionally and meticulously executed both his intrusion into TXClass and the extraction of a sizable quantity of confidential personal data." *Ibid.*

CONCLUSION

The petition for a writ of certiorari should be denied.

Respectfully submitted.

PAUL D. CLEMENT
Solicitor General

ALICE S. FISHER
Assistant Attorney General

MICHAEL A. ROTKER
Attorney

AUGUST 2007

No. 06-1602

In The

Supreme Court of the United States

CHRISTOPHER ANDREW PHILLIPS,

Petitioner,

v.

THE UNITED STATES OF AMERICA,

Respondent.

On Petition For A Writ Of Certiorari To The United States Court Of Appeals For The Fifth Circuit

REPLY BRIEF

TERRENCE W. KIRK
Texas Bar No. 11513500
502 West 13th Street
Austin, Texas 78701
(512) 236-8511
(512) 476-5346 (Fax)
Counsel for Petitioner

COCKLE LAW BRIEF PRINTING CO. (800) 225-6964
OR CALL COLLECT (402) 342-2831

TABLE OF CONTENTS

	Page
ADDRESS TO THE COURT	1
THE GOVERNMENT'S ARGUMENT	1
PETITIONER'S REPLY ARGUMENT	2
I. THIS COURT'S DECISION IN *CHAPMAN* DID NOT UNDERMINE ITS DECISION IN *STIRONE*	2
II. THIS COURT SHOULD NOT IGNORE THE CONFLICT IN THE CIRCUIT COURTS	4
III. THE FOURTH PRONG OF THE PLAIN-ERROR TEST IS NOT THE ISSUE HERE	8
CONCLUSION	11

TABLE OF AUTHORITIES

Page

CASES

Chapman v. California, 386 U.S. 18 (1967) 1, 2, 4

Neder v. United States, 527 U.S. 1 (1999) 4

Russell v. United States, 369 U.S. 749 (1962) 6

Stirone v. United States, 361 U.S. 212 (1960) 1, 2, 3, 4, 9

United States v. Brandao, 448 F. Supp. 2d 311 (D. Mass. 2006) 7

United States v. Brown, 400 F.3d 1242 (10th Cir. 2005) 4, 5

United States v. Cotton, 535 U.S. 625 (2002) ..... *passim*

United States v. Floresca, 38 F.3d 706 (4th Cir. 1994) (*en banc*) ..... *passim*

United States v. Griffin, 324 F.3d 330 (5th Cir. 2003) 5, 6

United States v. Magallanez, 408 F.3d 672 (10th Cir. 2005) 3

United States v. Milbourne, 129 Fed. Appx. 861 (4th Cir. 2005) 6

United States v. Mingo, ___ Fed. Appx. ___, 2007 WL 2301634 (4th Cir. 2007) 6

United States v. Murphy, 406 F.3d 857 (7th Cir. 2005), *cert. denied*, 546 U.S. 1097 (2006) 1, 2, 7

United States v. Olano, 507 U.S. 725 (1993) 4, 5

United States v. Rogers, 126 F.3d 655 (5th Cir. 1997) 3

TABLE OF AUTHORITIES – Continued

Page

United States v. Smith, 801 A. 2d 958 (D.C. 2002) 10

United States v. Thomas, 274 F.3d 655 (2d Cir. 2001) (*en banc*) 9

United States v. Torres, 901 F.2d 205 (2d Cir.), *cert. denied*, 498 U.S. 906 (1990) 3

STATUTES

18 U.S.C. § 1030 9

RULES

FED. R. CRIM. P. 52(a) 3

TO THE HONORABLE JUSTICES OF THE SUPREME COURT:

COMES NOW Petitioner Christopher Andrew Phillips, by and through his undersigned counsel, and respectfully submits this Reply Brief. Petitioner offers the following in reply to the Brief for the United States in Opposition:

THE GOVERNMENT'S ARGUMENT

In its brief in this case, the Government argues that the cases Petitioner cites are based on *Stirone v. United States*, 361 U.S. 212 (1960), but that *Stirone* was decided before *Chapman v. California*, 386 U.S. 18 (1967), which held that even constitutional errors are subject to a harm analysis. Brief for the United States at p. 11. According to the Government, this means that there is a "substantial question" whether the cases supporting Petitioner are still valid. *Id.*

Second, the Government urges that the Fourth Circuit should be given the chance to reconsider its decision in *United States v. Floresca*, 38 F.3d 706 (1994) (*en banc*) "in an appropriate case." Brief for the United States at p. 13. The Government asserts that the Fourth Circuit has not "addressed the rule of *Florseca*" since this Court's decision in *United States v. Cotton*, 535 U.S. 625 (2002), and asks that the lower courts be given more time to assess the effect of *Cotton* before this Court intervenes. *Id.* at p. 13, noting that this Court denied review in *United States*

v. Murphy, 406 F.3d 857 (7th Cir. 2005), *cert. denied*, 546 U.S. 1017 (2006). *Id.*

Finally, the Government contends that Petitioner cannot prevail in any event because the fourth prong of the plain-error standard has not been satisfied. *Id.* at p. 14. The evidence that Petitioner accessed a computer without authorization, the Government says, was "essentially uncontroverted"; a jury finding that Petitioner "transmitted" information necessarily included a finding that he "accessed" the computer. *Id.*

Petitioner now addresses these arguments in turn.

PETITIONER'S REPLY ARGUMENT

I. THIS COURT'S DECISION IN *CHAPMAN* DID NOT UNDERMINE ITS DECISION IN *STIRONE*.

It is certainly true, as the Government notes, that a constitutional error of the *Stirone* type could never have been harmless before *Chapman*. In *Stirone*, however, the defendant had objected at trial to the constructive amendment, *Stirone* at U.S. 271-72, so no question of "structural error" was presented, even if that concept had existed. This Court did not say that the error was reversible simply because it was a constitutional error, but focused on the harm caused by the error:

> The grand jury which found this indictment was satisfied to charge that Stirone's conduct interfered with interstate importation of sand. *But neither this nor any other court can know that the grand jury would have been willing to charge that Stirone's conduct would interfere with interstate exportation of steel from a mill later to be built with Rider's concrete.* And it cannot be said with certainty that with a new basis for conviction added, Stirone was convicted *solely* on the charge made in the indictment that the grand jury returned.

Stirone at 361 U.S. 217 (Emphasis added).

Moreover, to say that constitutional errors *can* be harmless is not to say that they *must* be harmless if no objection has been made. Indeed, several of the lower courts have suggested that the plain-error standard is relaxed when the error is a constitutional one. *See, e.g., United States v. Torres*, 901 F.2d 205, 228 (2d Cir.), *cert. denied*, 498 U.S. 906 (1990) (Constitutional errors "noticed more freely" under Rule 52(a)); *United States v. Rogers*, 126 F.3d 655, 658 (5th Cir. 1997) ("Increased scrutiny" given in plain-error review when "constitutional right is at stake"); *United States v. Magallanez*, 408 F.3d 672, 683 (10th Cir. 2005) (Plain-error test "applied less rigorously" where constitutional error alleged).

Finally, to the extent that the *Floresca* rule is characterized as "structural," Petitioner agrees with the Government that it appears inconsistent with the

plain-error rule established in *United States v. Olano*, 507 U.S. 725 (1973). The Government, however, has mischaracterized Petitioner's argument: Petitioner is not necessarily arguing that *Floresca* should be the law, but given that it and other decisions conflict with the Fifth Circuit's decision, this Court should grant review to say what the law is. Ironically, the Government makes the case for granting review with its recognition that there is a "substantial question" whether the lower courts analyzing constructive amendments have ignored the effect of *Chapman* and *Neder v. United States*, 527 U.S. 1 (1999). *See also United States v. Cotton*, *supra*, at 535 U.S. 625, 631 (citing *Stirone* only for the proposition that a defective indictment is a "jurisdictional" error, and rejecting that doctrine).

II. THIS COURT SHOULD NOT IGNORE THE CONFLICT IN THE CIRCUIT COURTS.

Unable to deny that the law is in flux as to whether a defendant must show prejudice under the plain-error doctrine, the Government wants the Court to ignore the conflict in the circuit courts. The Government apparently believes that the Fourth Circuit will eventually (sooner or later) come around to its point of view. After all, the Government observes, the Tenth Circuit has already abandoned its automatic reversal rule in *United States v. Brown*, 400 F.3d 1242, 1253, n. 6 (2005). Brief for the United States at pp. 14-15.

In *Brown*, however, the court did not decide the question presented here: must prejudice always be shown under the plain-error doctrine? Instead, the Tenth Circuit decided only, as this Court did in *Cotton*, that under the fourth prong of plain-error review, the defendant could not prevail because evidence of his guilt of the charged crime was "overwhelming." *Brown* at 400 F.3d 1254-55.

As will be seen, the Government wants to conflate the third and fourth prongs of *Olano*, and argue that Petitioner did not show "prejudice" here (the holding of the Fifth Circuit) because the evidence was allegedly so "overwhelming" that the Fifth Circuit, and this Court, would not have found the error serious enough to affect the fairness or integrity of the trial (a matter on which the Fifth Circuit did not rule, but which the Government wants this Court to decide in peremptory fashion).

What the Government overlooks is that an appellate court's approach to the prejudice issue may well affect its view of the fourth prong. If, for example, a court believes that no prejudice need be shown, or that there is a rebuttable presumption of prejudice, it may be more inclined to exercise its discretion and reverse a conviction.

The Fifth Circuit's decision in *United States v. Griffin*, 324 F.3d 330 (5th Cir. 2003), provides a useful example. In *Griffin*, the Fifth Circuit provided no analysis of the prejudice caused by an unobjected-to constructive amendment except to say that it could

not permit the district court to second guess "what was in the mind of the grand jury at the time it returned the indictment." *Id.* at 324 F.3d 355, quoting from this Court's decision in *Russell v. United States*, 369 U.S. 749, 770 (1962). To allow such an amendment, the court concluded, would violate the Fifth Amendment "and undermine the public's faith in the integrity of our judicial proceedings." *Id.*

This Fifth Circuit decision in 2003 appears to adopt the *Floresca* rule and at least assumes that no prejudice must be shown. And yet, just three years later in Petitioner's case, the Fifth Circuit applied a radically different standard, not even citing *Griffin*. Petitioner respectfully submits that where different panels of the same court are deciding the same issue in completely different ways, there can be no fairness.

Nor is it any answer to hope that things will just sort themselves out, without intervention by this Court. It may be literally true that the Fourth Circuit has not "addressed" the *Floresca* rule since *Cotton* was decided, but the Fourth Circuit has indicated at least twice, albeit in unpublished opinions, that it still approves of the *Floresca* rule. *See United States v. Milbourne*, 129 Fed. Appx. 861, 864 (4th Cir. 2005) (quoting *Floresca* rule but finding no constructive amendment); *United States v. Mingo*, ___ Fed. Appx. ___, 2007 WL 2301634 (4th Cir. 2007) ("Constructive amendments of a federal indictment. . . . are error *per se*.").

Finally, even if the *Floresca* court has the epiphany the Government anticipates, what of the other circuit courts? As the court observed in *United States v. Brandao*, 448 F. Supp. 311, 320-21 (D. Mass. 2006), the circuit courts are split into at least three camps on whether a defendant must show prejudice. The Fourth Circuit presumes prejudice, and holds that the error is *per se* reversible; the Second Circuit holds that prejudice has been shown *per se*; the Third Circuit "has crafted a middle-ground, holding that a rebuttable presumption of prejudice exists." *Brandao* at 448 F. Supp. 2d 320-21. And, of course, the Fifth Circuit apparently does what it wants to, but usually demands that the defendant show prejudice, as in Petitioner's case.

Petitioner cannot know, of course, why this Court denied review in *Murphy*, *supra*. Perhaps it was because the Petitioner there only pointed to the conflict between the Fourth and Seventh Circuits, or perhaps the Court at that time shared the Government's sanguine view that the Fourth Circuit would soon heal itself.

In any event, of course, the Court's denial of certiorari in *Murphy* is not an endorsement of the Seventh Circuit, or even a rejection of *Floresca*. The time has come to settle the debate, and only this Court can do it.

III. THE FOURTH PRONG OF THE PLAIN-ERROR TEST IS NOT THE ISSUE HERE.

The Government seeks to avoid review on the question presented, that of the need to show prejudice, by asserting that Petitioner is arguing in the alternative that "even if *Floresca* is no longer good law, the fourth prong of the plain-error standard is satisfied" because the evidence of the charged offense was not overwhelming. Brief for the States at p. 14. While Petitioner did assert that the evidence was not overwhelming, however, Pet. at p. 13, Petitioner observed that the Fifth Circuit, like this Court in *Cotton*, did not reach the fourth prong of the plain-error test. *Id.* Accordingly, even if the determination of the *fourth prong* might be "fact-bound," Brief for the United States at p. 14, the issue in this case is the *third prong,* i.e., a showing of prejudice.

Petitioner, therefore, is not arguing "in the alternative," and the Government's Brief is non-responsive. If the Fifth Circuit had simply declined to exercise its discretion here, a different question would be presented: whether *Cotton* dictates that a court should never exercise its discretion in the case of an unobjected-to constructive amendment (and, if it may, what considerations should guide it in deciding to exercise its discretion).

Petitioner submits that when the question is that of prejudice, the Court might want to look at the

evidence presented at trial, as it did in *Stirone*,[1] but the more important question is what the grand jury might have done. Following *Stirone*, several lower courts have concluded that prejudice is presumed because a reviewing court can never guess about this. *See, e.g., United States v. Thomas*, 274 F.3d 655, 670 (2d Cir. 2001) (*en banc*).

Perhaps, however, the Court might want to re-examine this assumption. In this case, for example, the indictment shows that the grand jury was presented with the entire factual basis constituting the alleged offense: the use of a "brute-force attack" program and an elaborate description of what Petitioner allegedly did. Presented with these facts, however, the grand jury indicted Petitioner only for "accessing," not "transmitting." Had the grand jury wanted to, it could have, of course, alleged both ways of violating 18 U.S.C. § 1030. It chose not to, even if one accepts the Government's notion that transmitting "information" constitutes "accessing."[2] Brief for

---

[1] The *Stirone* Court's second reason for finding harm was that the Court could not determine "with certainty" that Stirone was convicted "solely" on the charged offense. *Id.* at 361 U.S. 217. If that was true in *Stirone*, where both theories of the offense were submitted to the jury in the alternative, *id.* at 361 U.S. 272, how could that be any less true here, where the charged offense was not submitted to the jury at all?

[2] Not surprisingly, the Government cites no caselaw for the proposition that transmitting "information" constitutes accessing. Every time a Justice of this Court logs on to Westlaw, does he or she "transmit" information? And, if so, why have the "accessing" subsection at all? Not to mention, of course, that the

(Continued on following page)

the United States at p. 14, n. 7. *Cf. United States v. Smith*, 801 A. 2d 958, 962 (D.C. 2002) (Fourth prong not satisfied where evidence supported charged offense *and* "indictment included a citation that encompassed both subsections" of statute).

In short, the gravamen of a constructive amendment error is that it violates the defendant's right to be *charged by the grand jury*; the fact that the evidence may support the charged offense does not mean the grand jury would necessarily have indicted on the uncharged offense. Accordingly, while the quality of the proof at trial may constitute circumstantial evidence of what the grand jury might have done, the indictment may provide far better proof. At least for the purpose of determining prejudice, this Court should not adopt the *Cotton* test, which was intended to apply to a different prong of the plain-error test.

Fifth Circuit believed Petitioner had transmitted a "program," the theory actually argued to the jury, as opposed to the new one just appearing in the Government's brief.

CONCLUSION

It is up to the Government to indict the defendant before trial, not at the end of it. This Court should grant review to determine whether a failure to object relieves the Government of that duty where no objection is made at trial.

Respectfully submitted,

TERRENCE W. KIRK
Texas Bar No. 11513500
502 West 13th Street
Austin, Texas 78701
(512) 236-8511
(512) 476-5346 (Fax)
Counsel for Petitioner